



TITLE:

A Note on Hayden's Theorem(GROUPS AND COMBINATORICS)

AUTHOR(S):

Atsumi, Tsuyoshi

CITATION:

Atsumi, Tsuyoshi. A Note on Hayden's Theorem(GROUPS AND COMBINATORICS). 数理解析研究所講究録 1992, 794: 161-168

ISSUE DATE:

1992-06

URL:

<http://hdl.handle.net/2433/82729>

RIGHT:

A Note on Hayden's Theorem

Tsuyoshi Atsumi

厚見 寅司

The Case a finite Group G acts on Code.

1. Definitions from Coding Theory

Yoshida [5] showed that there is a generalization of MacWilliams identity [3] to codes with group action. We use ideas from [1] to give an elementary proof to Yoshida's identity in a special case.

Let V be the vector space \mathbf{F}_q^n , where \mathbf{F}_q is the field with q elements. From now on we assume that G is a finite permutation group on the coordinates of V and $|G|$ is prime to q . Then we can define a natural action of G on V as follows: If $\mathbf{v} = (v_1, \dots, v_n)$ and $g \in G$, we let $\mathbf{v}g = (x_1, \dots, x_n)$ where for $i = 1, \dots, n$, $x_i = v_{i_g-1}$. In this way V becomes an FG -module. A G -code is an FG -submodule of V . As in [1], the operator θ is defined by

$$\theta = \frac{1}{|G|} \sum_{g \in G} g.$$

Here we note that $C_V(G) = V\theta$ and $\theta^T = \theta$ (see [1]).

Let C_1, \dots, C_t be the orbits of the coordinates of V under the action of G . Let m_i be the orbit length of C_i . Define \bar{C}_i as the vector of V which has 1 as its entry for every point of C_i and 0 elsewhere. (This definition of the \bar{C}_i 's is slightly different from that in the proof of Theorem 4.3 in [1]). Then each of $\bar{C}_1, \dots, \bar{C}_t$ is in $U = V\theta$ and every element \mathbf{u} of $U = V\theta$ is of the form

$$\mathbf{u} = \sum_{i=1}^t x_i \bar{C}_i.$$

This basis $\{\bar{C}_1, \dots, \bar{C}_t\}$ of U is a key to our proof of Yoshida's result. Yoshida weight of a vector $\mathbf{u} = \sum_{i=1}^t x_i \bar{C}_i \in U$ denoted $wy(\mathbf{u})$ is defined as the number of non-zero x_i . So if G consists of the identity element, e , alone, then Yoshida weight $wy(\mathbf{u})$ of a vector \mathbf{u} is the ordinary weight $|\mathbf{u}|$. If $\mathbf{a} = \sum_{i=1}^t a_i \bar{C}_i$ and $\mathbf{b} = \sum_{i=1}^t b_i \bar{C}_i$ are any two vectors in U , then inner product $(\mathbf{a}, \mathbf{b})_G$ of \mathbf{a} and \mathbf{b} is defined by

$$(\mathbf{a}, \mathbf{b})_G = a_1 b_1 + \dots + a_t b_t. \quad (1)$$

Let D be a vector subspace of $U = V\theta$. D_G^\perp is the dual of D in U with respect to the inner product (1). (Notice that if G consists of the identity element, e , alone, then $D_{\{e\}}^\perp$ is the ordinary dual D^\perp of D in V .)

We describe a weight enumerator of a vector subspace D of $U = V\theta$. The weight enumerator $W_D(x, y)$ of D is defined by

$$W_D(x, y) = \sum_{u \in D} x^{t-wy(u)} y^{wy(u)}.$$

Clearly if G is trivial, that is, $G = \{e\}$, then this weight enumerator becomes the ordinary weight enumerator. For notation and terminology, we will refer the following book and paper: [3] for coding theory; [5] for codes with group action.

2. G-Codes

We have the following theorem which is a special case of Yoshida's result [5].

Theorem 1. *If C is a G -code, then*

$$W_{C^\perp\theta}(x, y) = \frac{1}{|C\theta|} W_{C\theta}(x + (q-1)y, x - y).$$

If G is trivial, that is, $G = \{e\}$, then our theorem is the ordinary MacWilliams theorem [3, pp 146]

In order to prove Theorem 1 we need the following proposition.

Proposition 1 (Hayden). *Let V be the vector space \mathbf{F}_q^n . Assume that G is a finite permutation group on the coordinates of V and $|G|$ is prime to q . If C is a G -code and*

$$\theta = \frac{1}{|G|} \sum_{g \in G} g,$$

then

$$(C\theta)^\perp = \text{Ker } \theta + C^\perp\theta.$$

Proof. See the proofs of Theorem 4.2 and Corollary 1 in [1]. ■

We will prove Theorem 1. If $\mathbf{x} = \sum_i x_i \bar{C}_i \in C\theta$ and $\mathbf{y} = \sum_i y_i \bar{C}_i \in C^\perp\theta$, by Proposition 1 we have

$$0 = (\mathbf{x}, \mathbf{y}) = \sum_i m_i x_i y_i = (\mathbf{x}, \mathbf{y}')_G,$$

where $\mathbf{y}' = \sum_i m_i y_i \bar{C}_i$. From this it follows that

$$(C\theta)^\perp \supseteq (C^\perp\theta)M, \tag{2}$$

where

$$M = \text{diag}(a_1, \dots, a_n) \quad i = 1, \dots, n;$$

$$a_i = m_j \quad \text{if } i \in C_j.$$

Next we will show that

$$(C\theta)^\perp_G \subseteq (C^\perp\theta)M. \quad (3)$$

If $\mathbf{x} = \sum_i x_i \bar{C}_i \in (C\theta)^\perp_G$, $\mathbf{x}' = \sum_i (x_i/m_i) \bar{C}_i$ and $\mathbf{y} = \sum_i y_i \bar{C}_i \in C\theta$, we have

$$(\mathbf{x}', \mathbf{y}) = \sum_i m_i (x_i/m_i) y_i = (\mathbf{x}, \mathbf{y})_G = 0.$$

This shows that

$$\mathbf{x}' \in (C\theta)^\perp. \quad (4)$$

Since $\mathbf{x}' \in U = V\theta$, (4) and Proposition 1 imply that $\mathbf{x}' \in C^\perp\theta$.

Hence, $\mathbf{x} = \mathbf{x}'M \in (C^\perp\theta)M$. Now we proved that

$$(C\theta)^\perp_G \subseteq (C^\perp\theta)M. \quad (5)$$

From (2) and (5) it follows that

$$(C\theta)^\perp_G = (C^\perp\theta)M. \quad (6)$$

Here notice that MacWilliams theorem [3. pp 146] for the ordinary weight enumerator of the code $C\theta$ in $U (= V\theta)$ holds in this case, too.

MacWilliams theorem.

$$W_{(C\theta)^\perp_G}(x, y) = \frac{1}{|C\theta|} W_{C\theta}(x + (q-1)y, x - y).$$

Now we will finish the proof of Theorem 1. By the above MacWilliams theorem and (6), we obtain the following.

$$W_{(C^\perp\theta)M}(x, y) = \frac{1}{|C\theta|} W_{C\theta}(x + (q-1)y, x - y). \quad (7)$$

Since $W_{(C^\perp\theta)M}(x, y) = W_{C^\perp\theta}(x, y)$, it follows from (7) that

$$W_{C^\perp\theta}(x, y) = \frac{1}{|C\theta|} W_{C\theta}(x + (q-1)y, x - y). \quad \blacksquare$$

Remark. Generalizing a result of Thompson, Hayden [1] has proved the following proposition.

Proposition 2. *Using the notation of Proposition 1, then with an appropriate orthonormal base for U , (extending \mathbf{F}_q if necessary) we have where $(C\theta)^\perp_U$ is the dual in terms of this basis*

$$(C\theta)^\perp_U = C^\perp \theta.$$

So our result (6) is a generalization of Proposition 2 in a sense.

The Case a finite Group G acts on Lattice

3. Definitions from Lattice Theory

In [5] Yoshida raised the following problem.

Problem. What can we say about lattices with groups action ? Can we define the equivariant version of theta functions?

He showed in [5] that there is a generalization of MacWilliams identity [3] to codes with group action. In this paper we will prove that there is a lattice version of this result. In order to state our theorem we introduce notation and terminology in lattice theory. Let V be the real n -dimensional space \mathbf{R}^n . A lattice Λ [4] is a subgroup of V satisfying one of the following equivalent conditions:

- i) Λ is discrete and V/Λ is compact;
- ii) Λ is discrete and generates the \mathbf{R} -vector space V ;
- iii) There exists an \mathbf{R} -basis (e_1, \dots, e_n) of V which is a \mathbf{Z} -basis of Λ (i.e. $\Lambda = \mathbf{Z}e_1 \oplus \dots \oplus \mathbf{Z}e_n$).

Let the coordinates of the basis vectors be

$$\begin{aligned} e_1 &= (e_{11}, \dots, e_{1n}), \\ e_2 &= (e_{12}, \dots, e_{2n}), \\ &\vdots \\ e_n &= (e_{1n}, \dots, e_{nn}). \end{aligned}$$

The $n \times n$ matrix M with (i, j) -entry equal to e_{ij} is called a generator matrix for Λ . The determinant of Λ is defined to be $\det \Lambda = |\det M|$. Given two vectors $\mathbf{u} = (u_1, \dots, u_n)$,

$\mathbf{v} = (v_1, \dots, v_n)$ of V , their inner product will be denoted by $\mathbf{u} \cdot \mathbf{v}$ or (\mathbf{u}, \mathbf{v}) . The dual lattice is defined by

$$\Lambda^\perp = \{\mathbf{u} \in \mathbf{R}^n \mid \mathbf{u} \cdot \mathbf{v} = u_1 v_1 + \dots + u_n v_n \in \mathbf{Z} \text{ for all } \mathbf{v} \in \Lambda\}.$$

The theta series $\Theta_\Lambda(z)$ of a lattice Λ is given by

$$\Theta_\Lambda(z) = \sum_{\mathbf{u} \in \Lambda} q^{\mathbf{u} \cdot \mathbf{u}},$$

where $q = e^{\pi i z}$. Jacobi's formula for the theta series of the dual lattice:

$$\Theta_{\Lambda^\perp}(z) = (\det \Lambda)(i/z)^{n/2} \Theta_\Lambda(-1/z). \quad (8)$$

The main purpose of this paper is to generalize equation (8) when a finite group G acts on Λ . From now on we assume that G is a finite permutation group on the coordinates of V . Then we can define a natural action of G on V as follows: If $\mathbf{v} = (v_1, \dots, v_n) \in V$ and $g \in G$, we let $\mathbf{v}g = (x_1, \dots, x_n)$ where for $i = 1, \dots, n$, $x_i = v_{i_{g^{-1}}}$. In this way V becomes an $\mathbf{R}G$ -module. A G -lattice is a lattice which is also an $\mathbf{Z}G$ -submodule of V . As in [1], the operator θ is defined by

$$\theta = \frac{1}{|G|} \sum_{g \in G} g.$$

Here we note that $V\theta = \{\mathbf{v} \in V \mid \mathbf{v}g = \mathbf{v} \text{ for all } g \in G\}$ and $\theta^T = \theta$ (see [1]).

Let C_1, \dots, C_t be the orbits of the coordinates of V under the action of G . Let m_i be the orbit length of C_i . Define \overline{C}_i as the vector of V which has $1/\sqrt{m_i}$ as its entry for every point of C_i and 0 elsewhere. (This definition of the \overline{C}_i 's is similar to that in the proof of Theorem 4.3 in [1]). Then each of $\overline{C}_1, \dots, \overline{C}_t$ is in $V\theta$ and every element \mathbf{u} of $V\theta$ is of the form

$$\mathbf{u} = \sum_{i=1}^t x_i \overline{C}_i.$$

If $\mathbf{a} = \sum_{i=1}^t a_i \overline{C}_i$ and $\mathbf{b} = \sum_{i=1}^t b_i \overline{C}_i$ are any two vectors in $V\theta$, then inner product $\mathbf{a} \circ \mathbf{b}$ of \mathbf{a} and \mathbf{b} is defined by

$$\mathbf{a} \circ \mathbf{b} = a_1 b_1 + \dots + a_t b_t. \quad (9)$$

Let D be a lattice in $V\theta$. D_G^\perp is the dual of D in $V\theta$ with respect to the inner product (9). The norm of $\mathbf{u} \in D$ is $\mathbf{u} \circ \mathbf{u}$.

We describe the theta series $\Theta_D(z)$ of a sublattice D as follows:

$$\Theta_D(z) = \sum_{\mathbf{u} \in D} q^{\mathbf{u} \circ \mathbf{u}},$$

where $q = e^{\pi iz}$.

For notation and terminology, we will refer the following book and paper: [4] for lattice theory; [5] for lattices with group action.

4. G-Lattices

We have the following:

Theorem 2. *If Λ is a G -lattice and $\Lambda_0 = \{\mathbf{r} \in \Lambda \mid \mathbf{r}\theta \in \Lambda\}$, then*

$$\Theta_{\Lambda_0^\perp \theta}(z) = (\det \Lambda_0 \theta)(i/z)^{n/2} \Theta_{\Lambda_0 \theta}(-1/z).$$

Note that $\Lambda_0 \theta = \Lambda \cap \Lambda \theta = \{\mathbf{v} \in \Lambda \mid \mathbf{v}g = \mathbf{v} \text{ for all } g \in G\}$.

In order to prove Theorem 2 we need the following proposition.

Proposition 3. *Let V be the vector space \mathbf{R}^n . Assume that G is a finite permutation group on the coordinates of V . If Λ is a G -lattice and $\Lambda_0 = \{\mathbf{r} \in \Lambda \mid \mathbf{r}\theta \in \Lambda\}$, then*

$$(\Lambda_0 \theta)^\perp = \text{Ker } \theta \oplus \Lambda_0^\perp \theta.$$

Proof. Our proof is similar to the proof of Theorem 4.2 in [1]. We note that Λ_0 is a G -sublattice of G -lattice Λ . If $\mathbf{r} \in \Lambda_0$, $\hat{\mathbf{r}} \in \Lambda_0^\perp$ and $\mathbf{y} \in \text{Ker } \theta^T (= \theta)$, we have

$$(\hat{\mathbf{r}}\theta^T, \mathbf{r}\theta) = (\hat{\mathbf{r}}, \mathbf{r}\theta^2) = (\hat{\mathbf{r}}, \mathbf{r}\theta) \in Z,$$

since $\mathbf{r}\theta \in \Lambda \cap \Lambda \theta \subseteq \Lambda_0$ and

$$(\mathbf{y}, \mathbf{r}\theta) = (\mathbf{y}\theta^T, \mathbf{r}) = 0 \in Z.$$

This shows that

$$\text{Ker } \theta + \Lambda_0^\perp \theta \subseteq (\Lambda_0 \theta)^\perp. \quad (10)$$

If $\mathbf{r} \in \Lambda_0$, $\mathbf{y} \in (\Lambda_0 \theta)^\perp$, we have

$$(\mathbf{y}\theta^T, \mathbf{r}) = (\mathbf{y}, \mathbf{r}\theta) \in Z.$$

So

$$\mathbf{y}\theta^T = \mathbf{y}\theta \in \Lambda_0^\perp.$$

Hence

$$\mathbf{y} = \mathbf{y} - \mathbf{y}\theta + (\mathbf{y}\theta)\theta \in \text{Ker } \theta + \Lambda_0^\perp \theta.$$

This implies that

$$(\Lambda_0\theta)^\perp \subseteq \text{Ker } \theta + \Lambda_0^\perp\theta. \quad (11)$$

(10) and (11) complete the proof of Proposition 3. ■

We will prove Theorem 2. If $\mathbf{x} = \sum_i x_i \overline{C}_i \in \Lambda_0\theta$ and $\mathbf{y} = \sum_i y_i \overline{C}_i \in \Lambda_0^\perp\theta$, by Proposition 3 we have

$$\mathbf{x} \circ \mathbf{y} = (\mathbf{x}, \mathbf{y}) \in Z.$$

So

$$\Lambda_0^\perp\theta \subseteq (\Lambda_0\theta)_G^\perp. \quad (12)$$

Now take $\mathbf{x} = \sum_i x_i \overline{C}_i \in (\Lambda_0\theta)_G^\perp$, $\mathbf{y} = \sum_i y_i \overline{C}_i \in \Lambda_0\theta$. and observe

$$(\mathbf{x}, \mathbf{y}) = \mathbf{x} \circ \mathbf{y} \in Z.$$

This shows that

$$\mathbf{x} \in (\Lambda_0\theta)^\perp. \quad (7)$$

Since $\mathbf{x} \in V\theta$, (13) and Proposition 3 imply that $\mathbf{x} \in \Lambda_0^\perp\theta$.

Now we proved that

$$(\Lambda_0\theta)_G^\perp \subseteq \Lambda_0^\perp\theta. \quad (14)$$

From (12) and (14) it follows that

$$(\Lambda_0\theta)_G^\perp = \Lambda_0^\perp\theta.$$

Now we will finish the proof of Theorem 2. Jacobi's formula for the theta series of the dual lattice $(\Lambda_0\theta)_G^\perp$ in $V\theta$:

$$\Theta_{(\Lambda_0\theta)_G^\perp}(z) = (\det \Lambda_0\theta)(i/z)^{n/2} \Theta_{\Lambda_0\theta}(-1/z).$$

Hence $(\Lambda_0\theta)_G^\perp = \Lambda_0^\perp\theta$ establishes our theorem. ■

Remark. It is easy to prove that

$$\begin{aligned} \Lambda/\Lambda_0 &\cong \Lambda\theta/\Lambda \cap \Lambda\theta, \\ \Lambda_0 &= (\Lambda \cap \text{Ker } \theta) \oplus (\Lambda \cap \Lambda\theta). \end{aligned}$$

References

- [1] W. G. Bridges, M. Hall, Jr. and J. L. Hayden , *Codes and Designs*, J. Combin. Theory Ser. A **31**(1981), 155–174.
- [2] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Springer-Verlag, New York-Berlin-Heidelberg-London-Paris-Tokyo, (1988).
- [3] F. J. MacWilliams and N. J. A. Sloane, *The Theory of The Error-Correcting Codes*, North Holland, Amsterdam-New York-Oxford, (1977).
- [4] J. P. Serre, *Cours d'Arithmétique*, Presses Universitaires de France, Paris, (1970); English translation, Springer-Verlag, New York-Berlin-Heidelberg-London-Paris-Tokyo, (1973).
- [5] T. Yoshida, *MacWilliams Identities for Linear Codes with Group Action*, Kyoto Univ. Inst. Math. Kōkyuroku, **671**(1988), 33–54.

Department of Mathematics
Faculty of Science
Kagoshima University
Kagoshima 890
Japan